The Structure and Properties of Binary Cyclic Alphabets

By JESSIE MacWILLIAMS

(Manuscript received July 8, 1964)

A code which is to be used for error control on a real data system is necessarily restricted by the nature of the transmitting equipment. These restrictions have no connection with the primary function of the code; indeed, they frequently eliminate most of the codes about which anything is known at present.

For example, the code to be used for error control by detection and retransmission on the trunks between data switching centers is required to be a cyclic (or truncated cyclic) code with 744 information places and 20 parity check bits. The computational problem in this case is to locate those cyclic codes which have exactly 20 parity checks and a block length of 764 or greater, and pick the one which is best suited for error control over a particular channel.

This paper outlines a procedure for attacking such problems. It describes how to locate the cyclic codes with a fixed block length and a fixed number of parity checks, if any such exist, and gives some methods of finding the number of code words of each weight in a particular code. If one knows the statistics of the channel it is then possible to estimate the error control properties of the code.

The procedure depends on an analysis of the algebraic structure of cyclic codes, which is given in Section II of this paper. Section I contains step-by-step instructions with no mathematical justification. It is hoped that the theory presented in Section II may be useful in other applications.

INTRODUCTION

In this paper the word alphabet denotes a systematic code — one in which each code word contains a certain fixed number, k, of *information* places, the contents of which are arbitrary, and a fixed number, $n - k$, of *parity check* places. Each parity check digit is the sum of the contents of a particular subset of the information places. The number n is called the *block length* of the alphabet. The individual members of the alphabet are called *letters*.

It is well known[1] that the letters of an alphabet of block length n form a subspace of the vector space of all possible rows of n binary symbols. This large space is denoted by V^n, V being the field 0, 1. The number of information places, k, is also the dimension of the subspace occupied by the alphabet.[1] A cyclic alphabet has the additional property that, if it contains a letter α, it contains as well every vector of V^n which is a cyclic permutation of α.

Cyclic alphabets are popular for error control for several good reasons. First, it is easy and relatively inexpensive to encode a cyclic alphabet. Second, the "best" known alphabets are cyclic alphabets.* Third, the cyclic property introduces a great deal of algebraic structure, which may be used to predict the error-detecting properties of the alphabet and to find alphahets with appropriate properties.

An alphabet to be used in a data transmission system must satisfy certain requirements. There will certainly be restrictions on tbe size of n and k, and one naturally requires also that the alphabet should be of some use for error control. These restrictions cannot be completely arbitrary; for a given pair of integers n, k there is likely to be no cyclic alphabet at all, let alone one with desirable error control properties.

The Hamming distance between two vectors is the number of coordinate places in which they differ. The distance between v_1 and v_2 is thus the minimum number of changes one would have to make in v_1 in order to convert it into v_2. The usual strategy for choosing an alphabet is to place its members as far apart as possible in terms of the Hamming distance. It would then require a relatively large number of errors to change a letter of the alphabet into another letter of the same alphabet.

The weight of a vector of V^n is its distance from the origin, which is the same as the number of ones it contains. Let α, of weight s, be a letter of an alphabet $\mathcal{A}$. If β is another letter of $\mathcal{A}$, so also is $\alpha + \beta$, since $\mathcal{A}$ is a vector space; $\alpha + \beta$ is at distance s from β. Let $A(s)$ denote the number of letters of $\mathcal{A}$ of weight s. $A(s)$ is then the numher of letters of $\mathcal{A}$ which are at distance s from an arbitrary letter of $\mathcal{A}$.

The set of numbers $A(0), \cdots, A(n)$ is called the spectrum of $\mathcal{A}$. The spectrum of $\mathcal{A}$, combined with the statistics of the channel, may be used to obtain an approximate estimate of the error control performance of the alphabet.[2]

An alphabet used for error detection will fail to detect an error pattern which is itself a letter of the alphabet. If $A(i) = 0$, the alphabet will

* The reason for this is very possibly that no other class of alphabets has been so systematically studied.

detect all $\binom{n}{i}$ patterns of i errors in a block of length n. If $A(i) \neq 0$, the alphabet will fail to detect $A(i)$ of these $\binom{n}{i}$ patterns. It is usual to require that $A(1)$ and $A(2)$ should be zero; it can be seen from analysis of the available data[2] that this makes good sense even on the telephone network. For larger values of i it would be fortunate if the letters of weight i were not the same as the most common error pattern, which is usually assumed to be a "burst." This assumption leads to the vaguely formulated requirement that letters of small weight should have their nonzero digits spread out as much as possible. A cyclic alphabet satisfies this requirement to a certain extent, since the letters of smallest weight must spread over at least $n - k + 1$ adjacent places.

Since it may actually become necessary to choose particular alphabets for error control purposes, and since that the requirements which these alphabets will have to satisfy are not yet known, it is desirable to be able to obtain some rather detailed information about available alphabets. This paper describes a computer-assisted procedure by which one may locate the cyclic alphabets which have values of n and k within certain bounds, and find the spectra of these alphabets. A considerable library of computer programs which are useful in this procedure has been developed.

The plan of the paper is as follows:

Section I contains step-by-step instructions for locating cyclic alphabets and finding their spectra.

Section II contains the mathematical justification for the procedures of Section I, and is in fact a fairly complete account of the structure of cyclic alphabets.

It is not necessary to read Section II in order to follow the recipes given in Section I. However, in a troublesome case — which means a case that involves a large expenditure of computer time — the material in Section II may suggest a way out of the difficulty.

I. PROPERTIES OF CYCLIC ALPHABETS

In this section we outline a procedure to attack the following problem:

Given that the block length, n, and the number of parity checks, m, of a binary cyclic alphabet are required to lie in the ranges

$$N_1 \leqq n \leqq N_2, \qquad M_1 \leqq m \leqq M_2,$$

find the alphabet (or alphabets) which have the greatest minimum distance.

It is assumed throughout that *n is an odd number*. Many of the propositions quoted in this section, and justified in Section II, are not true for even values of n.

Let $\mathfrak{R}_n$ be the ring of polynomials mod $x^n - 1$ over the binary field. $\mathfrak{R}_n$ consists of all polynomials of degree $\leqq n - 1$ with coefficients in the binary field. Addition of polynomials is done as usual; to multiply two polynomials, we multiply in the normal way and then reduce exponents of x mod n.

A cyclic alphabet of block length n may be regarded as a set $\mathfrak{A}$ of polynomials of $\mathfrak{R}_n$, with the property that every polynomial of $\mathfrak{A}$ is divisible (mod $x^n - 1$) by a fixed polynomial $a(x)$. $a(x)$ may, and will, be taken to be a factor of $x^n - 1$; then the number of parity checks for $\mathfrak{A}$ is the degree of $a(x)$. $a(x)$ will be called the *generating factor* of $\mathfrak{A}$. We write $\mathfrak{A} = \mathfrak{R}_n \cdot a(x)$.

Let ω stand for one of the numbers $0, 1, \cdots, n - 1$. Denote by $\Sigma_2(n)$ the permutation $\omega \to 2\omega$ mod n. $\Sigma_2(n)$ divides the integers $0, 1, \cdots, n - 1$ into a number of disjoint cycles; the cycles of $\Sigma_2(63)$, for example, are shown in Table I.

Let $f_0(x), f_1(x), \cdots, f_{t-1}(x)$ be the irreducible factors of $x^n - 1$. Since n is odd, these factors are all distinct. Let ζ be a primitive nth root of unity. The cycles of $\Sigma_2(n)$ and the polynomials $f_i(x)$ are associated in the following way: The zeros of $f_i(x)$ in a suitable* extension field of the binary field are $\zeta^{r_1}, \zeta^{r_2}, \cdots, \zeta^{r_k}$, where $(r_1, r_2, \cdots, r_k)$ is a cycle of $\Sigma_2(n)$; and each cycle represents in this way the zeros of one of the $f_i(x)$. The number of irreducible factors of $x^n - 1$ is, of course, the same as the number of cycles of $\Sigma_2(n)$. We say that the polynomial $f_i(x)$ with zeros $\zeta^{r_1}, \zeta^{r_2}, \cdots, \zeta^{r_k}$ is associated with the cycle $(r_1, r_2, \cdots, r_k)$.

Let S be a set of cycles of $\Sigma_2(n)$; let $f_{i_1}, \cdots, f_{i_r}$ be the irreducible factors of $x^n - 1$ which are associated with the cycles of S. Let

$$a(x) = f_{i_1}(x) \cdot f_{i_2}(x) \cdot \cdots \cdot f_{i_r}(x)$$

be the generating factors of an alphabet $\mathfrak{A}$. We say that the cyclic alphabet $\mathfrak{A} = \mathfrak{R}_n \cdot a(x)$ is associated with the set S.

Let $1 < r_1 < r_2 < \cdots < n$ be a list of the factors of n. Attach to each cycle of $\Sigma_2(n)$ an *exponent* $e_i = n/r_i$ defined by the property that each member of the cycle is divisible by r_i mod n, and that r_i is the largest factor of n for which this is true.

A great deal of information about the cyclic alphabets of block length n can be obtained by looking at the cycles of $\Sigma_2(n)$.

* For example, the Galois field of order 2^t, consisting of the roots of $y^{2^t} = y$, where t is the length of the cycle of $\Sigma_2(n)$ which contains 1. A proof of this "well-known" correspondence is given in Section II.

TABLE I — CYCLES OF $\Sigma_2(63)$

Cycles						Exponent
1	2	4	8	16	32	63
3	6	12	24	33	48	21
5	10	17	20	34	40	63
7	14	28	35	49	56	9
9	18	36				7
11	22	25	37	44	50	63
13	19	26	38	41	52	63
15	30	39	51	57	60	21
21	42					3
23	29	43	46	53	58	63
27	45	54				7
31	47	55	59	61	62	63
0						1

Proposition I: Let $\eta_0, \eta_1, \cdots, \eta_{t-1}$ be the cycles of $\Sigma_2(n)$ and let m_i be the length of η_i. The number of cyclic alphabets of block length n is 2^t. The alphabet associated with a set S of cycles has $m = \sum_{\eta_i \epsilon S} m_i$ parity checks.*

Proposition II: Let e be the least common multiple of the exponents of the cycles contained in S. If $e < n$ the alphabet associated with S has minimum distance 2. If $e = n$ the minimum distance of the alphabet is at least 3.

Proposition III (Bose-Chaudhuri Bound)*: If S contains the numbers* $1, 2, 3, \cdots, d - 1, d$ *among its cycles, the minimum distance of the alphabet associated with S is $\geqq d + 1$.*

It should be noted that the minimum distance may be, and often is, larger than the lower bounds given in propositions 2 and 3.

At this point one may, of course, be forced to conclude that there are no satisfactory cyclic alphabets of block length n. The main purpose of propositions 1 and 2 is to eliminate useless values of n. Suppose, however, that we have a value of n for which there exist alphabets with the required number of parity checks and of minimum distance at least 3. It is then useful to establish a 1-1 correspondence between the cycles of $\Sigma_2(n)$ and the irreducible factors of $x^n - 1$.

The exponent of a polynomial $f(x)$ is the least value of e for which $f(x)$ divides $x^e - 1$. We find the irreducible factors of $x^n - 1$,† and of $x^{c_i} - 1$, $(c_i = n/a_i)$ for each factor a_i of n. Some of the irreducible fac-

* This number includes three "trivial" alphabets: the alphabet consisting of all of $\mathcal{R}_n$, the alphabet containing only zero, and the alphabet containing only zero and the vector of weight n.

† This has, in fact, been done for all odd values of $n \leqq 1023$.

tors of $x^n - 1$ have exponent e_i; these appear among the irreducible factors of $x^{e_i} - 1$, and can be identified by inspection.

Any irreducible factor of $x^n - 1$ which has exponent n can be chosen to correspond to the cycle of $\Sigma_2(n)$ which contains 1. Let $f_1(x)$ be this polynomial; $f_1(x)$ has ζ as a zero. If r is a proper factor of n, r is the least member of a cycle of exponent $e = n/r$. The polynomial associated with this cycle also has exponent e. Let $g_1, g_2, \cdots, g_s$ be the irreducible factors of $x^n - 1$ with exponent e. By picking $f_1(x)$ to correspond to the cycle containing 1, we have implicitly chosen which of the $g_i(x)$ corresponds to the cycle containing r. The choice can be made explicit in the following way:

*Proposition IV: $g_i(x^r)$ is exactly divisible by $f_1(x)$ if and only if it corresponds to the cycle containing r.**

We can now assign to each factor r_i of n an irreducible factor f_i of $x^n - 1$, which will have exponent $e_i = n/r_i$. We have not yet matched every cycle of $\Sigma_2(n)$ with an irreducible factor of $x^n - 1$; the remaining work will be done by a different method. Before describing this we illustrate the procedure so far.

Suppose that the restrictions on n, m are $52 \leqq n \leqq 64$, $m = 9$. It is found that

$\Sigma_1(53)$ has two cycles, lengths 1, 52
$\Sigma_2(55)$ has five cycles, lengths 1, 4, 10, 20, 20
$\Sigma_2(57)$ has five cycles, lengths 1, 2, 18, 18, 18
$\Sigma_2(59)$ has two cycles, lengths 1, 58
$\Sigma_2(61)$ has two cycles, lengths 1, 60
$\Sigma_2(63)$ has thirteen cycles, lengths 1, 2, 3, and 6.

By Proposition I, 63 is the only possible block length, since the lengths of the cycles of the other numbers do not add up to nine. The factors of 63 are 3, 7, 9, 21. The cycles of $\Sigma_2(63)$ and their exponents are shown in Table I. The nine parity checks are obtained by taking a cycle of length 6 and a cycle of length 3 or a cycle of length 6 and the cycles of length 2 and 1. By Proposition II, the least common multiple of the exponents of the cycles should be 63; hence the cycle of length 6 should have exponent 63 or 9.† The Bose-Chaudhuri bound provides no information; a minimum distance of three is guaranteed by Proposition II, and we cannot assemble a collection of cycles containing the numbers 1, 2, 3 with only nine parity checks. Hence we are faced with the possibility of having to compute the spectra of 18 different alphabets. (It will be shown later that this is not necessary.)

* This elegant and time-saving device was suggested by Mr. R. L. Graham.
† This case will be omitted because the author did not notice it in time.

Suppose that m is allowed to be 12; we pick the first and second cycles, because Proposition III then guarantees a minimum distance of at least five.*

Table II contains a list of irreducible factors of $x^{63} - 1$ and their exponents. Associate the first polynomial (714) with the first cycle. One of the polynomials of exponent 21 then corresponds to the second cycle; by Proposition IV we find that 534 is the correct choice. For the sake of completeness we use Proposition IV again to ascertain that the polynomial 640 corresponds to the cycle beginning with 9. The unique polynomials of exponent 9 and 3 must, of course, correspond to the cycles beginning with 7 and 21.

TABLE II — IRREDUCIBLE FACTORS OF $x^{63} - 1$

	Factor	Exponent	Associated Cycle
f_1	714	63	1, 2, 4, 8, 16, 32
f_2	414	63	
f_3	700	3	21, 42
f_4	554	63	
f_5	534	21	3, 6, 12, 24, 33, 48
f_6	634	63	
f_7	444	9	7, 14, 28, 35, 49, 56
f_8	664	63	
f_9	724	21	
f_{10}	604	63	
f_{11}	600	1	
f_{12}	540	7	
f_{13}	640	7	9, 18, 36

The polynomials are in octal, which stands for a binary number denoting the positions of the nonzero coefficients. The least exponent is on the left, e.g.

$$714 = 111001100 = 1 + x + x^2 + x^5 + x^6.$$

To explain the next steps it is necessary to introduce some more definitions.

Let q be an integer prime to n. The mapping $\sigma_q : x^j \rightarrow x^{qj}$ (exponents mod n) is an automorphism of $\mathfrak{R}_n$. The effect of σ_q on a cyclic alphabet is to change it into an equivalent[1] cyclic alphabet; $\mathfrak{A}\sigma_q = \mathfrak{A}'$, and $\mathfrak{A}$, $\mathfrak{A}'$ have the same spectrum. The number of σ_q which have a different effect on $\mathfrak{A}$ is rather small; if q_1, q_2 are in the same cycle of $\Sigma_2(n)$, then

$$\mathfrak{A}\sigma_{q_1} = \mathfrak{A}\sigma_{q_2}.$$

(In particular if q is in the cycle which contains 1, $\mathfrak{A}\sigma_q = \mathfrak{A}$.)

* It is not established mathematically that a different choice cannot give a greater minimum distance. To be completely safe we should calculate the spectra of all alphabets with 12 parity checks and exponent 63.

We select one q out of each cycle of $\Sigma_2(n)$ which contains numbers prime to n. For $n = 63$ we choose the numbers underlined in Table I; this choice is computationally advantageous, since $5^2 = 25 \bmod 63$, $5^3 = 62 \bmod 63$, $5^4 = 58 \bmod 63$, $5^5 = 38 \bmod 63$.

Every cyclic alphabet of $\mathcal{A}$ contains a unique polynomial $c(x)$, the *idempotent* of $\mathcal{A}$ which has the useful property that $\mathcal{A}\sigma_q = \mathcal{A}'$ if and only if $c(x)\sigma_q = c'(x)$. For computational purposes it is much better to know the idempotent of $\mathcal{A}$ than the generating factor of $\mathcal{A}$. The idempotent of the alphabet $\mathcal{R}_n \cdot f_i(x)$, where $f_i(x)$ is an irreducible factor of $x^n - 1$, is denoted by $1 + \theta_i(x)$. The polynomials $\theta_i(x)$, $i = 1, 0, \cdots, t - 1$ are called the primitive idempotents of $\mathcal{R}_n$, and have several useful properties:

(*i*) The $\theta_i(x)$ are easy to compute, and in fact have been computed for all odd values of $n \leqq 1023$. (The method by which this is done is described in the next section.)

(*ii*) The idempotent of the alphabet with generating factor $f_{i_1}(x)\, f_{i_2}(x) \cdot \cdots \cdot f_{i_r}(x)$ is

$$1 + \theta_{i_1}(x) + \theta_{i_2}(x) + \cdots + \theta_{i_r}(x).$$

(*iii*) The $\theta_i(k)$ are permuted among themselves by the automorphisms σ_q.

The alphabet with idempotent $\theta_i(x)$ is a *minimal* alphabet of $\mathcal{R}_n$ (t contains no subalphabet except 0). Its generating factor is $(x^n - 1)/f_i(x)$. The alphabet with generating factor $f_i(x)$ has generating idempotent $1 + \theta_i(x)$ and is a maximal alphabet of $\mathcal{R}_n$.

In the future the cyclic alphabet $\mathcal{A}$ will be identified by a sum of primitive idempotents of $\mathcal{R}_n$ rather than by a product of irreducible factors of $x^n - 1$.

Proposition V: If $f_1(x)$, $f_2(x)$ are irreducible factors of $x^n - 1$ with the same exponent, then $\theta_1(x)\sigma_q = \theta_2(x)$ for some automorphism σ_q of R_n. Hence the minimal alphabets generated by $\theta_1(x)$, $\theta_2(x)$ are equivalent, and the maximal alphabets generated by $1 + \theta_1(x)$, $1 + \theta_2(x)$ are also equivalent. Conversely, if two minimal (maximal) alphabets have the same spectrum, they are equivalent under one of the automorphisms σ_q.

Proposition VI: The alphabet with idempotent $(1 + \theta_{i_1} + \cdots + \theta_{i_r})$ is equivalent to the alphabet with idempotent $(1 + \theta_{i_1}\sigma_q + \cdots + \theta_{i_r}\sigma_q)$.

Proposition VII: Let $1 + \theta_i(x)$ be the idempotent associated with the cycle of $\Sigma_2(n)$ which contains 1. Let u, v be integers prime to n such that $u \cdot v \equiv 1 \bmod n$. Then $1 + \theta_i(x)\sigma_u$ is the idempotent associated with the cycle which contains v.

We illustrate again for the case $n = 63$. Table III contains a list of primitive idempotents of $\mathcal{R}_{63}$. This list is parallel to the list in Table II.

TABLE III – PRIMITIVE IDEMPOTENTS OF $\mathfrak{R}_{63}$

			Associated Cycle	
			From Table II	From Prop. 6
θ_1	321026251170	156307227	1, 2, 4, 8, 16, 32	
θ_2	010305172162	267315277		11, 22, 25, 37, 44, 50
θ_3	333333333333	333333333	21, 42	
θ_4	044160277124	317353233		5, 10, 17, 20, 34, 40
θ_5	012231301223	130122313	3, 6, 12, 24, 33, 48	
θ_6	375343166036	225150213		31, 47, 55, 56, 61, 62
θ_7	044044044044	044044044	7, 14, 28, 35, 49, 56	
θ_8	331327363052	375016044		22, 29, 43, 46, 53, 58
θ_9	323112032311	203231120		15, 30, 39, 51, 57, 60
θ_{10}	375263355116	136243020		13, 19, 26, 38, 41, 52
θ_{11}	777777777777	777777777	0	
θ_{12}	456271345627	134562713		27, 45, 54
θ_{13}	723516472351	647235164	9, 18, 36	

The ith factor, $f_i(x)$ of Table II, is the generating factor of the alphabet with idempotent $1 + \theta_i(x)$ where $\theta_i(x)$ is the ith primitive idempotent of Table III. We associate some of the θ_i with a cycle of $\Sigma_2(63)$ by copying from Table II.

The automorphism σ_5 produces the following permutation of the set of primitive idempotents of $\mathfrak{R}_{63}$

$$(\theta_1, \theta_{10}, \theta_8, \theta_6, \theta_2, \theta_4)\ (\theta_5, \theta_9)\ (\theta_{12}, \theta_{13})(\theta_3)\ (\theta_7)\ (\theta_{11}).$$

The other automorphisms, as already noted, produce powers of this permutation; for example $\sigma_{62} = \sigma_{5^3}$ gives

$$(\theta_1, \theta_6)\ (\theta_{10}, \theta_2)\ (\theta_8, \theta_4)\ (\theta_5, \theta_9)\ (\theta_{12}, \theta_{13})\ (\theta_3)\ (\theta_7)\ (\theta_{11}).$$

Consider now the alphabet with nine parity checks which is associated with the cycles (1, 2, 4, 8, 16, 32) and (9, 18, 36). By Table II the generating factor of this alphabet is $f_1(x) \cdot f_{13}(x)$; its idempotent is $(1 + \theta_1 + \theta_{13})$. The idempotents which can be obtained from this by the permutations σ_5 and its powers are

$$1 + \theta_{10} + \theta_{12},\ 1 + \theta_8 + \theta_{13},\ 1 + \theta_6 + \theta_{12},\ 1 + \theta_2 + \theta_{13},\ 1 + \theta_4 + \theta_{12}.$$

The generating factors of the corresponding alphabets are (including the original alphabet),

$$f_1 \cdot f_{13},\ f_{10} \cdot f_{12},\ f_8 \cdot f_{13},\ f_6 \cdot f_{12},\ f_2 \cdot f_{13},\ f_4 \cdot f_{12}.$$

By Proposition VI these six alphabets are all equivalent. Similarly, the alphabet associated with cycles (1, 2, 4, 8, 16, 32) and (27, 45, 54) has

idempotent $1 + \theta_1 + \theta_{12}$, and is equivalent to the alphabets with idempotents

$$1 + \theta_{10} + \theta_{13}, \; 1 + \theta_8 + \theta_{12}, \; 1 + \theta_6 + \theta_{13}, \; 1 + \theta_2 + \theta_{12}, \; 1 + \theta_4 + \theta_{13}.$$

The third possibility for nine parity checks consists of the cycles (1, 2, 4, 16, 32), (21, 42), (0). The associated idempotent is $1 + \theta_1 + \theta_3 + \theta_{11}$; equivalent alphabets are given by the idempotents

$$1 + \theta_{10} + \theta_3 + \theta_{11}, \; 1 + \theta_8 + \theta_3 + \theta_{11}, \; 1 + \theta_6 + \theta_3 + \theta_{11},$$
$$1 + \theta_2 + \theta_3 + \theta_{11}, \; 1 + \theta_4 + \theta_3 + \theta_{11}.$$

Hence, among the 18 alphabets with nine parity checks and minimum distance $\geqq 3$, there are actually at most three different spectra.

We observed before that the alphabet with twelve parity checks associated with cycles (1, 2, 4, 8, 16, 32) and (3, 6, 12, 24, 33, 34) has minimum distance at least 5. The idempotent of this alphabet is $1 + \theta_1 + \theta_5$. There are at least* five equivalent alphabets with idempotents

$$1 + \theta_{10} + \theta_9, \; 1 + \theta_8 + \theta_5, \; 1 + \theta_6 + \theta_9, \; 1 + \theta_2 + \theta_5, \; 1 + \theta_4 + \theta_9.$$

It may very well happen that one of these alphabets is easier to instrument than our original choice.

The 1-1 correspondence between cycles of $\Sigma_2(63)$ and primitive idempotents of $\mathfrak{R}_{63}$ is completed by Proposition VII, and entered in Table IV. For example, $5 \cdot 38 = 190 = 1 \bmod 63$ ($38 = 5^5 \bmod 63$); hence

$$\theta_1\sigma_5 = \theta_{10}$$

corresponds to the cycle (13, 19, 26, 38, 41, 52).

It is now necessary to face the problem of actually computing the spectrum of a cyclic alphabet.

For a small alphabet this can be done by counting, without too large an expenditure of computer time. An alphabet of block length 765 with 2^{20} letters can be examined, a letter at a time, in 0.32 hours on a 7094. This alphabet has 745 parity checks. Typically, however, one wishes to know the spectrum of the alphabet with 2^{745} letters and 20 parity checks; to compute this by counting would take over a million computer years. Fortunately there is a way out of this dilemma.

Let $a(x)$, of degree m, be a factor of $x^n - 1$, and let

$$b(x) = (x^n - 1)/a(x).$$

* It is entirely possible that alphabets not contained in this list also have the same spectrum, and are perhaps equivalent to the first alphabet under a permutation which is not an automorphism of $\mathfrak{R}_n$.

TABLE IV — SPECTRA OF SMALL ALPHABETS OF R_{63}

$\theta_1 + \theta_{12}$ 2^9 letters
$B(0) = 1$
$B(28) = 189$
$B(32) = 252$
$B(36) = 7$
$B(40) = 63$
$\theta_1 + \theta_{13}$ 2^9 letters
$B(0) = 1$
$B(28) = 252$
$B(32) = 63$
$B(36) = 196$
$\theta_1 + \theta_3 + \theta_{11}$ 2^9 letters
$B(0) = 1$
$B(25) = 3$
$B(26) = 63$
$B(29) = 126$
$B(31) = 63$
$B(32) = 63$
$B(34) = 126$
$B(37) = 63$
$B(42) = 3$
$B(63) = 1$
$\theta_1 + \theta_5$ 2^{12} letters
$B(0) = 1$
$B(24) = 210$
$B(28) = 1512$
$B(32) = 1071$
$B(36) = 1176$
$B(40) = 126$

The alphabets $\mathcal{A} = \mathcal{R}_n \cdot a(x)$ and $\mathcal{B} = \mathcal{R}_n \cdot b(x)$ are called dual or orthogonal alphabets.* Let $A(s)$, $B(s)$ be the number of letters of weight s in $\mathcal{A}$, $\mathcal{B}$. We suppose that $\mathcal{A}$ with m parity checks is a large alphabet, whose spectrum we wish to find; $\mathcal{B}$ contains 2^m letters, and its spectrum can be found by counting or by more sophisticated procedures. The $A(s)$ can be found from the $B(s)$ by the following proposition.[3]

Proposition VIII: The quantities $A(s)$, $B(s)$ are related by the expression

$$2^m \sum_{s=0}^{n} A(s) z^s = \sum_{s=0}^{n} B(s)\ (1+z)^{n-s}(1-z)^s.$$

* This is not quite the usual definition; the usual dual alphabet of $\mathcal{A}$ is equivalent to $\mathcal{B}$, so has the same spectrum. The difference is explained fully in Section II.

We now describe methods which are sometimes useful for finding the spectra of small cyclic alphabets.

Let α be a letter of a cyclic alphabet $\mathcal{A}$, and let αT be the letter obtained from α by one cyclic permutation to the right. For example, for $n = 7$ one might have

$$\alpha = (0\ 1\ 1\ 0\ 1\ 1\ 1), \qquad \alpha T = (1\ 0\ 1\ 1\ 0\ 1\ 1),$$
$$\alpha T^2 = (1\ 1\ 0\ 1\ 1\ 0\ 1) \text{ etc.}$$

The letters αT^ν all belong to $\mathcal{A}$. The set of distinct letters αT^ν for fixed α is called a cycle of $\mathcal{A}$; α is a representative of this cycle; the number of distinct letters is $\pi(\alpha)$, the period of α or the length of the cycle. Knowing the length of each cycle of $\mathcal{A}$ and the weight of a letter from each cycle, we can at once compute the spectrum of $\mathcal{A}$.

If $\mathcal{A}$, $\mathcal{B}$ are dual alphabets, and the idempotent of $\mathcal{A}$ is $1 + c(x)$, then $c(x)$ is the idempotent of $\mathcal{B}$. The alphabet $\mathfrak{M}_i$ with idempotent $\theta_i(x)$ is the dual of the maximal alphabet with irreducible generating factor $f_i(x)$. $\mathfrak{M}_i$ is called a minimal alphabet. The alphabet with generating factor $f_i(x)f_j(x)$ has idempotent $1 + \theta_i(x) + \theta_j(x)$; its dual alphabet is the union of $\mathfrak{M}_i$ and $\mathfrak{M}_j$ and has idempotent $\theta_i(x) + \theta_j(x)$. The procedure is to find cycle representatives for the $\mathfrak{M}_i$ and then put them together to get cycle representatives for $\mathfrak{M}_i \cup \mathfrak{M}_j$. This is done by the following propositions.

Proposition IX: Every cycle (except that containing the zero letter) of $\mathfrak{M}_i$ has length $\pi(\theta_i)$; further $\pi(\theta_i)$ is the exponent, e_i, of the irreducible polynomial $f_i(x)$.

For example, for $n = 63$, $\mathfrak{M}_1$ has one cycle of length 63. This cycle contains the letter corresponding to $\theta_1(x)$, which has weight 32; the spectrum of $\mathfrak{M}_1$ is $B(0) = 1$, $B(32) = 63$. The spectrum of the maximal alphabet $\mathcal{R}_{63} \cdot f_1(x)$ is given by

$$2^6 \sum_{s=0}^{63} A(s) z^s = (1 + z)^{63} + 63(1 + z)^{31}(1 - z)^{32}.$$

Similarly $\mathfrak{M}_{12}$ has one cycle of length 7 which contains the letter corresponding to $\theta_{12}(x)$, of weight 36. The spectrum of $\mathfrak{M}_{12}$ is $B(0) = 1$, $B(36) = 7$, and the dual alphabet $\mathcal{R}_{63} \cdot f_{12}(x)$ has the spectrum $A(s)$ given by

$$2^3 \sum_{s=0}^{63} A(s) z^s = (1 + z)^{63} + 7(1 + z)^{27}(1 - z)^{36}.$$

We note that

$$8A(2) = \binom{63}{2} + 7\left[\binom{27}{2} - 27\cdot 36 + \binom{36}{2}\right] = 2016,$$

agreeing with the statement of Proposition II that this particular alphabet will contain letters of weight 2.

The alphabet $\mathfrak{M}_5$ contains three cycles of length 21. It is possible to check by hand that θ_5, $\theta_5 + \theta_5 T$ and $\theta_5 + \theta_5 T^2$ are in different cycles; their weights are 24, 36 and 36, respectively; the spectrum of $\mathfrak{M}_5$ is $B(0) = 1$, $B(24) = 21$, $B(36) = 42$.

The technique is useful only if $\mathfrak{M}_i$ contains a rather small number of different cycles; otherwise the process of finding cycle representatives becomes extremely laborious.

Once the cycle representatives for $\mathfrak{M}_i$ and $\mathfrak{M}_j$ are known, one constructs cycle representatives for the alpbabet $\mathfrak{M}_i \cup \mathfrak{M}_j$ (with idempotent $\theta_i + \theta_j$) by the following proposition.

Proposition X: Let $\mathfrak{M}_i$ have cycle representatives $m_1, m_2, \cdots, m_\alpha$, of period e_i, and $\mathfrak{M}_j$ have cycle representatives $n_1, n_2, \cdots, n_\beta$, of period e_j. Let H, h be the least common multiple and highest common factor of e_i, e_j. Then $\mathfrak{M}_i \cup \mathfrak{M}_j$ has cycle representatives $m_1, \cdots, m_\alpha, n_1, \cdots, n_\beta$, and in addition, for each pair i, j, cycle representatives $m_i + n_j T^\nu$, $\nu = 0, 1, \cdots, h - 1$ of period H.

For example, for $n = 63$ the alphabet $\mathfrak{M}_1 \cup \mathfrak{M}_{12}$ has one cycle representative θ_1 (period 63), one cycle representative θ_{12} (period 7), and 7 cycle representatives $\theta_1 + \theta_{12} T^\nu$, $\nu = 0, 1, \cdots, 6$ of period 63. The alphabet $\mathfrak{M}_1 \cup \mathfrak{M}_{13}$ is constructed similarly. The spectrum of the alphabet

$$\mathfrak{M}_1 \cup \mathfrak{M}_3 \cup \mathfrak{M}_{11}$$

is obtained by constructing that of $\mathfrak{M}_1 \cup \mathfrak{M}_3$ (cycle representatives θ_1, θ_3, $\theta_1 + \theta_3$, $\theta_1 + \theta_3 T$) and adding the letter of weight 63 represented by θ_{11}. The spectra of these three alphabets and their duals are given in Tables IV and V. The dual alphabets are the three nonequivalent alphabets of block length 63 and with nine parity checks which we set out to find.

The alphabet $\mathfrak{M}_1 \cup \mathfrak{M}_5$ has cycle representatives θ_1, period 63, θ_5, $\theta_5 + \theta_5 T$, $\theta_5 + \theta_5 T^2$, period 21, and $\theta_1 + \theta_5 T^\nu$, $\theta_1 + (\theta_5 + \theta_5 T)T^\nu$, $\theta_1 + (\theta_5 + \theta_5 T^2)T^\nu$, $\nu = 0, 1, \cdots, 20$. The spectra of this alphabet and its dual are given in Tables IV and V; the dual alphabet has minimum distance 5 as predicted.

We now give a summary of the procedure:

(1) Obtain a list of the cycles of $\Sigma_2(n)$ for each allowable value of n, and check to see whether an allowable number of parity checks can be

TABLE V — SPECTRAL PROBABILITIES* OF LARGE ALPHABETS OF R_{63}

$1 + \theta_1 + \theta_{12}$ (9 parity checks)

$$
\begin{aligned}
a(0) &= 1 = a(63)\\
a(1) &= a(2) = a(3) = 0;\\
a(4) &= 0.21153 \times 10^{-2},\\
a(5) &= 0.20973 \times 10^{-2},\\
a(6) &= 0.19243 \times 10^{-2},\\
a(7) &= 0.19571 \times 10^{-2},\\
a(8) &= 0.19526 \times 10^{-2},\\
a(s) &= a(n - s)\\
a(s) &= 2^{-9} \text{ for other values of } s.
\end{aligned}
$$

$1 + \theta_1 + \theta_{13}$ (9 parity checks)

$$
\begin{aligned}
a(0) &= 1 = a(63)\\
a(1) &= a(2) = 0\\
a(3) &= a(4) = 0.15865 \times 10^{-2},\\
a(5) &= a(6) = 0.20077 \times 10^{-2},\\
a(7) &= a(8) = 0.19451 \times 10^{-2},\\
a(9) &= a(10) = 0.19544 \times 10^{-2},\\
a(11) &= a(12) = 0.19528 \times 10^{-2},\\
a(s) &= a(n - s)\\
a(s) &= 2^{-9} \text{ for other values of } s.
\end{aligned}
$$

$1 + \theta_1 + \theta_3 + \theta_{11}$ (9 parity checks)

$$
\begin{aligned}
a(0) &= 1\\
a(1) &= a(2) = a(3) = 0,\\
a(4) &= 0.19634 \times 10^{-2}\\
a(6) &= 0.19626 \times 10^{-2}\\
a(8) &= 0.19502 \times 10^{-2}\\
a(i) &= 0 \text{ all odd values of } i\\
a(2i) &= 2^{-9} \text{ other values of } i.
\end{aligned}
$$

$1 + \theta_1 + \theta_5$ (12 parity checks)

$$
\begin{aligned}
a(0) &= 1 \quad a(63) = 1\\
a(1) &= a(2) = a(3) = a(4) = 0,\\
a(5) &= a(6) = 0.26889 \times 10^{-3},\\
a(7) &= a(8) = 0.24119 \times 10^{-3},\\
a(9) &= a(10) = 0.24461 \times 10^{-3},\\
a(11) &= a(12) = 0.24404 \times 10^{-3},\\
a(13) &= a(14) = 0.24416 \times 10^{-3},\\
a(s) &= a(n - s)\\
a(s) &= 2^{-12} \text{ other values of } s.
\end{aligned}
$$

* The spectral probability $a(s)$ is $A(s)/\binom{n}{s}$; the number $A(s)$ is frequently too large for the computer.

obtained as the sum of lengths of distinct cycles. Discard the values of n for which this is not possible.

(2) Attach an exponent to each cycle of $\Sigma_2(n)$.

Let S be a set of cycles of suitable lengths. Find the least common multiple of the exponents of the cycles in S. Discard the sets S for which this number is less than n.

(3) It is now necessary to set up a correspondence between the cycles of S and the primitive idempotents of $\mathfrak{R}_n$. This is done in two steps, as follows. Obtain a list of the irreducible factors of $x^n - 1$, and of $x^{e_i} - 1$, $e_i = n/r_i$ for each proper factor r_i of n. Let $f_0(x), f_1(x), \cdots, f_{t-1}(x)$ be the irreducible factors of $x^n - 1$. The irreducible factors of $x^{e_i} - 1$ will be among the $f_i(x)$. Starting with the smallest value of e_i, attach an exponent to each of the $f_i(x)$ by comparing lists. Pick any $f_i(x)$ of exponent n to correspond to the cycle beginning with 1, and using Proposition IV, find the polynomial of exponent e_i, which then corresponds to the cycle beginning with r_i.

(4) Obtain a parallel list of primitive idempotents of $\mathfrak{R}_n$, and transfer to this the cycles whose position in the correspondence has been found. Pick an integer q from each cycle of $\Sigma_2(n)$ which contains numbers prime to n, and find the effect of the permutation σ_q on the set of primitive idempotents. Use Proposition VII to complete the correspondence between cycles and primitive idempotents.

(5) Let $s_1, s_2, \cdots, s_\nu$ be the cycles of an allowable set S, $f_1(x), \cdots, f_\nu(x)$ the corresponding irreducible factors of $x^n - 1$, and $\theta_1(x), \cdots, \theta_\nu(x)$, the corresponding primitive idempotents. The desired alphabet has the generating factor $f(x) = f_1(x)f_2(x) \cdots f_\nu(x)$. The orthogonal alphabet has the generating idempotent

$$\theta(x) = \theta_1(x) + \theta_2(x) + \cdots + \theta_\nu(x).$$

Divide the allowable alphabets into automorphism classes by looking at the effect of the automorphisms σ_q on the idempotent $\theta(x)$. Alphabets in the same automorphism class have the same spectrum.

(6) The orthogonal alphabet $\mathfrak{R}_n \cdot \theta(x)$ is frequently much smaller than the desired alphabet $\mathfrak{R}_n \cdot f(x)$. In this case it is advantageous to compute the spectrum of $\mathfrak{R}_n \cdot \theta(x)$ and to obtain the spectrum of $\mathfrak{R}_n \cdot f(x)$ from this by Proposition VIII. If $\theta(x)$ is the sum of two or three primitive idempotents, its spectrum may be built up in the way described in Proposition X. Otherwise the alphabet may be generated by the vectors corresponding to polynomials $\theta(x), x\theta(x), \cdots, x^m\theta(x)$ [m = degree of $f(x)$], and the spectrum obtained by counting.

II. PROOFS

In this section we give the proofs of the propositions of the first section.

Let V be the binary field, and V^n the set of all possible rows of n binary symbols. V^n is a vector space of dimension n over V. Let $\mathfrak{R}_n$ be, as before, the set of polynomials mod $x^n - 1$ over V. $\mathfrak{R}_n$ is a commutative ring.

We may relate V^n and $\mathcal{R}_n$ hy (1-1) mapping

$$\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \leftrightarrows \alpha_0, \alpha_1, \cdots, \alpha_{n-1}.$$

This mapping clearly preserves addition in hoth $\mathcal{R}_n$ and V^n.

A subset $\mathcal{A}$ of polynomials of $\mathcal{R}_n$ is an ideal if

(*i*) $g_1, g_2 \in \mathcal{A} \Rightarrow g_1 + g_2 \in \mathcal{A}$,
(*ii*) $g \in \mathcal{A} \Rightarrow rg \in \mathcal{A}$ for any $r \in \mathcal{R}_n$.

An ideal in $\mathcal{R}_n$ corresponds by property (*i*) to a linear suhspace of V^n. By property (*ii*), with $r = x$, this suhspace in invariant under a cyclic permutation of coordinates, hence is a cyclic alphabet in V^n. Conversely a cyclic alphabet in V^n is an ideal in $\mathcal{R}_n$. We represent both ideal and alpbabet by the same symbol, $\mathcal{A}$.

Lemma 2.0: An ideal $\mathcal{A}$ of $\mathcal{R}_n$ consists of all multiples (in $\mathcal{R}_n$) of a polynomial $a(x)$ which divides $x^n - 1$. $a(x)$ is the unique polynomial of least degree in $\mathcal{A}$.*

The proof of this lemma can be found in Peterson,[4] section 6.4.

$a(x)$ will he called the *generating factor* of $\mathcal{A}$. The polynomial $b(x) = (x^n - 1)/a(x)$ will he called the *reciprocal factor* of $\mathcal{A}$. This notation is used throughout; the ideal named $\mathcal{A}$ always has a generating factor named $a(x)$ and a reciprocal factor named $b(x)$. The degree of $a(x)$ will he denoted by m, and that of $b(x)$ hy k; of course $m + k = n$.

Lemma 2.1: The dimension of $\mathcal{A}$ as a vector space of V^n is k; the number of parity checks for the alphabet $\mathcal{A}$ is m. For proof, see Peterson,[4] theorem 6.11.

The numher of different alphahets of $\mathcal{R}_n$ is the number of different factors of $x^n - 1$; the dimension of alphahet $\mathcal{A}$ is the degree of its reciprocal factor. However, if n is odd, (which we always assume) one can find which dimensions are availahle in hlock length n without going to the considerable trouhle of finding all the factors of $x^n - 1$.

Let ω stand for one of the numbers $0, 1, \cdots, n - 1$. Let $\Sigma_2(n)$ denote the mapping $\omega \rightarrow 2\omega \bmod n$. Since n is odd, this mapping is a permutation of the numhers $0, 1, \cdots, n - 1$.

The permutation $\Sigma_2(n)$ on $0, 1, \cdots, n - 1$ factors into a numher of cycles; the cycles of $\Sigma_2(63)$ are shown in Tahle I, Section I. It is a fairly trivial matter to find these cycles.

The relation hetween the cycles of $\Sigma_2(n)$ and the factors of $x^n - 1$ over V is a well-known part of Galois theory. It is descrihed in detail here only because of the difficulty of finding a concise reference.

* $a(x)$ divides $x^n - 1$ in the ring $V[x]$ of all polynomials over V. It is meaningless to say that something divides $x^n - 1$ in $\mathcal{R}_n$.

Lemma 2.2: Let S be a subset of the integers $0, 1, \cdots, n - 1$. S is invariant under $\Sigma_2(n)$ if and only if it is the union of a number of cycles of $\Sigma_2(n)$.

Proof: If S is such a union it is invariant under $\Sigma_2(n)$, since each separate cycle is invariant.

Suppose S to be invariant under $\Sigma_2(n)$ and let r belong to S. Then $2^\nu r$ also belongs to S for any value of ν. S contains with r the whole cycle containing r. Thus S is a union of cycles of $\Sigma_2(n)$.

Lemma 2.3: Let S be invariant under $\Sigma_2(n)$, and let S_t be the set of all sums $r_{s_1} + r_{s_2} + \cdots + r_{s_\tau}$, $r_{s_i} \epsilon S$, $r_{s_i} \neq r_{s_j}$. Then S_τ is invariant under $\Sigma_2(n)$.

Proof: We need show only that $\Sigma_2(n)$ maps S_τ into itself; the mapping must then be 1-1. Let $r_{s_1} + r_{s_2} + \cdots + r_{s_\tau} \epsilon S_\tau$; applying $\Sigma_2(n)$ we obtain $2r_{s_1} + 2r_{s_2} + \cdots + 2r_{s_\tau}$, which is again in S_τ. Hence the lemma is proved.

Let $(1,2,2^2, \cdots, 2^{m_1-1})$ be the cycle of $\Sigma_2(n)$ which contains 1. $2^{m_1} \equiv 1 \bmod n$, or n divides $2^{m_1} - 1$. Set $N = 2^{m_1} - 1$. Every nth root of unity is also an Nth root of unity. Let $V(2^{m_1})$ be the Galois field of the Nth roots of unity over the prime field V. $x^n - 1$ factors into linear factors over $V(2^{m_1})$ and these factors are of the form $x - \zeta^\nu$, where ζ is a primitive nth root of unity. (ζ is not a primitive Nth root of unity unless $n = N$.)

The automorphisms of $V(2^{m_1})$ over V are given by $\alpha \to \alpha^2$ and its powers, where $\alpha \epsilon V(2^{m_1})$; further, $\alpha = \alpha^2$ if and only if $\alpha \epsilon V$.[5]

The explicit connection between the cycles of $\Sigma_2(n)$ and the factors of $x^n - 1$ is as follows:

Lemma 2.4: Let $S = r_1, r_2, \cdots, r_m$ be a set of integers invariant under $\Sigma_2(n)$, with $r_i \neq r_j$. The polynomial $f(x) = \pi(x - \zeta^{r_i})$ has coefficients in V, and is a factor of $x^n - 1$ over V.*

Let $f(x) = (x - \zeta^{r_1}) \cdots (x - \zeta^{r_m})$ be the factorization over $V(2^{m_1})$ of a polynomial $f(x)$ which divides $x^n - 1$ over V. The set $r_1, r_2, \cdots, r_m$ is then invariant under $\Sigma_2(n)$.

Proof: Let $S = r_1, r_2, \cdots, r_m$ be a set of distinct integers which is invariant under $\Sigma_2(n)$. $f(x) = (x - \zeta^{r_1}) \cdots (x - \zeta^{r_m})$ divides $x^n - 1$ over $V(2^{m_1})$ since each linear factor divides $x^n - 1$, and $r_i \neq r_j$. Let $a_{n-\tau}$ be the coefficient of $x^{n-\tau}$ in $f(x)$. $a_{n-\tau}$ is the τth symmetric function of $\zeta^{r_1}, \cdots, \zeta^{r_m}$, or

$$a_{n-\tau} = \sum_{\substack{s_i \epsilon S \\ s_i \neq s_j}} \zeta^{r_{s_1} + \cdots + r_{s_\tau}}.$$

* Note again that we are working in $V[x]$, not in $\mathfrak{R}_n$.

$$(a_{n-\tau})^2 = \sum_{\substack{s_i \in S \\ s_i \neq s_j}} \zeta^{2r_{s_1}+\cdots+2r_{s_\tau}} = a_{n-\tau} \text{ by 2.3.}$$

Thus the coefficients of $f(x)$ are in V, and $f(x)$ divides $x^n - 1$ over V.

Suppose that $f(x)$ divides $x^n - 1$ over V. The zeros of $f(x)$ in $V(2^{m_1})$ are $\zeta^{r_1}, \zeta^{r_2}, \cdots, \zeta^{r_m}$ where ζ is a primitive nth root of unity, and $r_1, \cdots, r_m$ are integers mod n. Since by Lemma 2.3 all the symmetric functions of $\zeta^{r_1}, \zeta^{r_2}, \cdots, \zeta^{r_m}$ are in V, the transformation $\zeta \rightarrow \zeta^2$ preserves $f(x)$, and must be simply a permutation of the zeros of $f(x)$. Thus the set $r_1, r_2, \cdots, r_m$ is invariant under $\Sigma_2(n)$.

The smallest sets which are invariant under $\Sigma_2(n)$ are the individual cycles of $\Sigma_2(n)$. Each such cycle determines, in the way described above, the zeros of an irreducible factor of $x^n - 1$; each irreducible factor of $x^n - 1$ corresponds in this way to a cycle of $\Sigma_2(n)$.

Proof of Proposition I

The number of cycles of $\Sigma_2(n)$ is t, and, by the above, t is also the number of irreducible factors of $x^n - 1$. These irreducible factors are all different [$(x^n - 1)$ has no multiple roots over V if n is odd], and can be combined by multiplication to give 2^t different factors of $x^n - 1$. Further, these are all the factors of $x^n - 1$. Hence there are 2^t cyclic alphabets of block length n. Let $a(x) = f_1(x) \cdots f_\nu(x)$ be the generating factor of the cyclic alphabet $\mathfrak{A}$. Let m_i be the degree of $f_i(x)$. m_i is the length of the cycle of $\Sigma_2(n)$ corresponding to $f_i(x)$. By Lemma 2.1 the number of parity checks for $\mathfrak{A}$ is $m = \sum_{i=1}^{\nu} m_i$.

The exponent of a polynomial $a(x)$ is the least integer e such that $a(x)$ divides $x^e - 1$. Let

$$a(x) = (x - \zeta^{r_1}) \cdots (x - \zeta^{r_m}),$$

where ζ is a primitive nth root of unity, and $r_1, \cdots, r_m$ is a set of cycles of $\Sigma_2(n)$. The exponent of $a(x)$ is then the least value of e such that

$$(\zeta^{r_i})^e = 1, \quad \text{or} \quad er_i \equiv 1 \bmod n, \qquad i = 1, \cdots, m.$$

$e = n/\alpha$ where α is the greatest common factor of $r_1, \cdots, r_m$ and n.

If $a(x)$ is an irreducible factor of $x^n - 1$ [$r_1, \cdots, r_m$ is a single cycle of $\Sigma_2(n)$], the quantity α is the largest factor of n which divides each member of the cycle $r_1, \cdots, r_m$. $e = n/\alpha$ is said to be the exponent of the cycle as well as of the polynomial $a(x)$.

The exponent of a union of cycles or of a product of irreducible polynomials is the least common multiple of their individual exponents.

Proof of Proposition II

The ideal $\mathfrak{A}$ with generating factor $a(x)$ contains tbe polynomial $x^e - 1$ $(= x^e + 1)$, where e is the exponent of $a(x)$. If $e = n$, tbis polynomial is the zero of $\mathfrak{A}$; if $e < n$, it corresponds to a letter of weight 2 in the alpbabet $\mathfrak{A}$.

If $\mathfrak{A}$ contains a letter of weigbt 2, the ideal $\mathfrak{A}$ contains, by suitable cyclic permutation, a polynomial $x^e - 1$, $e < n$, which is divisible by $a(x)$; the exponent of $a(x)$ is then less than n.

Thus $\mathfrak{A}$ contains letters of weight 2 if and only if its generating factor has exponent less than n.

Proposition III is a restatement of the Bose-Cbaudhuri theorem; a proof can be found in Peterson,[4] Theorem 9.1.

There is considerable freedom of cboice in setting up an exact correspondence between cycles of $\Sigma_2(n)$ and irreducible factors of $x^n - 1$. This occurs because there are several primitive nth roots of unity; if ζ is one such, then so also is ζ^ν, where ν is any integer prime to n.

We pick any irreducible polynomial of exponent n to correspond to the cycle $(1, 2, \cdots, 2^{m-1})$. If this is to make sense, the alphabets generated by irreducible polynomials with the same exponent should be indistinguishable for our purposes. In fact they are equivalent;[1] this will be proved later.

The choice of a polynomial to correspond to the cycle $(1, 2, \cdots, 2^{m-1})$ implicitly fixes the exact correspondence between cycles of $\Sigma_2(n)$ and irreducible factors of $x^n - 1$. It remains to make this correspondence explicit, preferably by calculations involving only numbers in the prime field V. This is done in two stages, the first of which is given by Proposition IV.

Proof of Proposition IV

Let $f_1(x)$ be the polynomial chosen to correspond to tbe cycle $(1, 2, \cdots, 2^{m-1})$. Over the field $V(2^m)$ $f_1(x)$ factors into $(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{2^{m-1}})$. Let r be a factor of n and $\{g_i(x)\}$ the set of irreducible factors of $x^n - 1$ of exponent $e = n/r$. One of the $g_i(x)$ bas ζ^r as a zero over $V(2^m)$, and corresponds to the cycle containing r. This $g_i(x)$ can be identified by the following lemma.

Lemma 2.5: $g_i(x^r)$ is divisible by $f_1(x)$ over V if and only if $g_i(x)$ has ζ^r as a zero over $V(2^m)$.

Proof: Let $g(x)$ be any polynomial of exponent e. Since $g(x)$ divides $x^e - 1$ over V, $g(x^r)$ divides $x^{er} - 1 = x^n - 1$. $g(x^r)$ is a product of irreducible factors of $x^n - 1$.

Let $\alpha_0, \alpha_1, \cdots, \alpha_{s-1}$ be tbe cycle associated with $g(x)$, so that a typical factor of $g(x^r)$ is $(x^r - \zeta^{\alpha_i})$. The cycle $\beta_0, \beta_1, \cdots, \beta_{m-1}$ is associated witb $g(x^r)$ if and only if $r\beta_j = \alpha_i$ $[(\zeta^{\beta_j})^r = \zeta^{\alpha_i}]$ for a suitable choice of i,j.

Suppose now that $g_i(x^r)$ is divisible for $f_1(x)$ over V. Tbe cycle 1, 2, $\cdots$, 2^{m-1} is tben associated witb $g_i(x^r)$, and $\zeta^r = \zeta^{\alpha_i}$ for some i; thus ζ^r is a zero of $g_i(x)$.

Suppose tbat ζ^r is a zero of $g_i(x)$. The cycle associated with $g_i(x)$ is then $r, 2r, \cdots, 2^{s-1}r$. Clearly, 1, 2, $\cdots$, 2^{m-1} is a cycle associated with $g_i(x^r)$, and $f_1(x)$ divides $g_i(x^r)$.

It may be noted that the proof of this theorem provides a way of finding the factors of $g(x^r)$ whicb is useful in other applications.

Automorphisms and Idempotents of $\mathfrak{R}_n$

Let q be an integer prime to n, and let σ_q be the mapping of $\mathfrak{R}_n$ onto itself defined by $h(x) \to h(x^q)$, exponents reduced mod n where necessary. σ_q clearly preserves addition and multiplication in $\mathfrak{R}_n$, and is 1-1, since with q prime to n, $x^{iq} = x^{jq}$ implies $iq \equiv jq \bmod n$, implies $i \equiv j \bmod n$. σ_q is an automorphism of $\mathfrak{R}_n$, and $\mathfrak{A}\sigma_q$ is again an ideal.

In V^n, σ_q is a permutation of coordinate places, described by $\omega \to q\omega \bmod n$ [$\Sigma_2(n)$ is the special case σ_2]. Thus σ_q changes alphabets of V^n into equivalent alphabets, and in particular changes cyclic alphabets into equivalent cyclic alphabets.

The automorphisms σ_q are useful because it is easy to compute their effect on the ideals of $\mathfrak{R}_n$.

Lemma 2.6: Every ideal* $\mathfrak{A}$ *of* $\mathfrak{R}_n$ *contains a unique polynomial* $c(x)$ *with the following properties:*

(*i*) $c(x) = c(x)^2$; $c(x)$ *is idempotent*

(*ii*) $\mathfrak{A} = \mathfrak{R}_n \cdot c(x)$; $c(x)$ *generates* $\mathfrak{A}$

(*iii*) $c(x)$ *is a unit for* $\mathfrak{A}$.

(*iv*) $c(x)\sigma_q$ *is the idempotent of* $\mathfrak{A}\sigma_q$.

Proof: Let $a(x)$, $b(x)$ be the generating factor and reciprocal factor of $\mathfrak{A}$. Since n is odd, they are relatively prime. There exist polynomials $h_1(x)$, $h_2(x)$ such that $h_1(x)a(x) + h_2(x)b(x) = 1$, and $h_1(x)$, $h_2(x)$ are relatively prime to $b(x)$, $a(x)$, respectively. We show that $c(x) = h_1(x)a(x)$ is the idempotent of $\mathfrak{A}$.

(*i*) $c(x)^2 + c(x)h_2(x)b(x) = c(x)$. The second term on the left is zero since it contains the factor $x^n - 1$. Hence $c(x)$ is idempotent.

* In other words, $\mathfrak{R}_n$ is a commutative, semisimple ring. It is, of course, the group algebra over V of the cyclic group of order n; n odd implies that it is semisimple.[6]

(*ii*) The generating factor of the ideal $\mathfrak{R}_n \cdot c(x)$ is the highest common factor of $c(x)$ and $x^n - 1$. This is $a(x)$ by the construction of $c(x)$. Hence $\mathfrak{R}_n \cdot c(x) = \mathfrak{A}$.

(*iii*) If $\alpha(x) \in \mathfrak{A}$, $\alpha(x) = \alpha'(x)c(x)$ by (*ii*). Then $\alpha(x)c(x) = \alpha'(x)c(x)^2 = \alpha'(x)c(x)$ [by (*i*)] $= \alpha(x)$. Hence $c(x)$ is a unit for $\mathfrak{A}$. $c(x)$ is then necessarily unique, since the commutative ring $\mathfrak{A}$ cannot have two unities.

(*iv*) $c(x)\sigma_q$ is idempotent because σ_q is an automorphism of $\mathfrak{R}_n$, and is the unique idempotent of the ideal $\mathfrak{R}_n c(x)\sigma_q = \mathfrak{A}\sigma_q$.

We now associate with each ideal $\mathfrak{A}$ a third polynomial $c(x)$, the generating idempotent of $\mathfrak{A}$.

Corollary 2.7: $\mathfrak{A}\sigma_q = \mathfrak{A}$ if and only if $c(x)\sigma_q = c(x)$.

Corollary 2.8: $\mathfrak{A}\sigma_2 = \mathfrak{A}$ for every ideal $\mathfrak{A}$ of $\mathfrak{R}_n$; equivalently, the permutation $\Sigma_2(n)$ preserves every cyclic alphabet of V^n.

Two vectors $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$, $(\beta_0, \beta_1, \cdots, \beta_{n-1})$ are said to be orthogonal if

$$\sum_{i=0}^{n-1} \alpha_i \cdot \beta_i = 0 \text{ (multiplication and addition in } V).$$

The orthogonal complement (dual alphabet) $\mathfrak{A}^\perp$ of $\mathfrak{A}$ consists of the vectors of V^n which are orthogonal to every vector of $\mathfrak{A}$. For our purposes it is convenient to say that cyclic alphabets $\mathfrak{A}$, $\mathfrak{B}$ are orthogonal if $\mathfrak{B}$ is generated by $b(x) = (x^n - 1)/a(x)$. This is justified by the following lemma.

Lemma 2.9: $\mathfrak{A}^\perp$ is equivalent to the ideal generated by $b(x)$ and is obtained from it by the transformation $x \to x^{-1}$.

The proof of this lemma can be found in Peterson[4] (6.12).

Lemma 2.10: If $\mathfrak{A}$ has idempotent $c(x)$, the ideal $\mathfrak{B} = \mathfrak{R}_n \cdot b(x)$ has idempotent $1 + c(x)$.

Proof: By 2.6 the idempotent of $\mathfrak{B}$ is

$$h_2(x)b(x) = 1 + h_1(x)a(x) = 1 + c(x).$$

Since we have agreed to say that $\mathfrak{A}$, $\mathfrak{B}$ are orthogonal ideals, we may also say that $c(x)$, $1 + c(x)$ are orthogonal idempotents. This is fortunate, since it is a well-established convention in the theory of algebras to say that two idempotents are orthogonal if their product is zero.[6] [$c(x)(1 + c(x)) = c(x) + c(x) = 0$.] We shall adopt this convention. It is to be noted that orthogonality for ideals is still not the same as orthogonality for idempotents. The idempotents $c_1(x)$, $c_2(x)$ are orthogonal if $c_1(x) \cdot c_2(x) = 0$. The ideals they generate are not orthogonal unless also $c_1(x) + c_2(x) = 1$.

Lemma 2.11: (*i*) *The ideal* $\mathfrak{A}_1 \cap \mathfrak{A}_2$ *has idempotent* c_1c_2. (*ii*) *The ideal* $\mathfrak{A}_1 \cup \mathfrak{A}_2$ *has idempotent* $c_1 + c_2 + c_1c_2$.

Proof:

(*i*) $\mathfrak{A}_1 \cap \mathfrak{A}_2$ is generated by the least common multiple of $a_1(x)$, $a_2(x)$, say $\bar{a}(x)$. $\bar{a}(x)$ is tbe highest common factor of $c_1(x)c_2(x)$ and $x^n - 1$; hence $c_1(x)c_2(x)$ is the idempotent of the ideal $\mathfrak{R}_n \cdot \bar{a}(x)$.

(*ii*) Set $d(x) = c_1(x) + c_2(x) + c_1(x)c_2(x)$. The $c_1(x)d(x) = c_1(x)$, $c_2(x)d(x) = c_2(x)$. Thus $d(x)$ is idempotent, and the ideal $\mathfrak{R}_n d(x)$ contains $\mathfrak{A}_1$ and $\mathfrak{A}_2$.

Let $\bar{\mathfrak{A}}$ be any ideal which contains $\mathfrak{A}_1$ and $\mathfrak{A}_2$, and let $\bar{c}(x)$ be the idempotent of $\bar{\mathfrak{A}}$. Since $\bar{c}(x)$ is a unit for $\bar{\mathfrak{A}}$, $c_i(x)\bar{c}(x) = c_i(x)$, $i = 1, 2$. Then $d(x)\bar{c}(x) = d(x)$, and $\mathfrak{R}_n d(x)$ is contained in every ideal $\bar{\mathfrak{A}}$. Hence $\mathfrak{R}_n \cdot d(x) = \mathfrak{A}_1 \cup \mathfrak{A}_2$.

An ideal of $\mathfrak{R}_n$ is said to be a minimal ideal if it contains no subideal other than (0). A minimal ideal of $\mathfrak{R}_n$ will be denoted by $\mathfrak{M}_i$, its generating factor by $m_i(x)$, its reciprocal factor by $f_i(x)$, and its generating idempotent by $\theta_i(x)$. The idempotent of a minimal ideal is called a *primitive* idempotent.

Lemma 2.12:

(*i*) $\mathfrak{M}_i$ *is a minimal ideal if and only if* $f_i(x)$ *is an irreducible factor of* $x^n - 1$.

(*ii*) $\mathfrak{M}_i \cap \mathfrak{M}_j = 0$ *if* $i \neq j$; *the dimension of* $\mathfrak{M}_i \cup \mathfrak{M}_j$ *is the sum of the dimensions of* $\mathfrak{M}_i$ *and* $\mathfrak{M}_j$.

(*iii*) *Any ideal* $\mathfrak{A}$ *is the union of the minimal ideals continued in* $\mathfrak{A}$. *In particular,* $\mathfrak{R}_n$ *is the union of all its minimal ideals.*

Proof:

(*i*) follows from 2.1, since the dimension of a minimal ideal is as small as possible.

(*ii*) The generating factor of the ideal orthogonal to $\mathfrak{M}_i \cap \mathfrak{M}_j$ is the higbest common factor of $f_i(x)$ and $f_j(x)$, which is 1. Hence $\mathfrak{M}_i \cap \mathfrak{M}_j$ is equivalent to $\mathfrak{R}_n^{\perp}$ and is zero. The second statement follows immediately.

(*iii*) Let $b(x)$ be the reciprocal polynomial of $\mathfrak{A}$, and let $b(x) = f_1(x)f_2(x) \cdots f_\nu(x)$ where (since n is odd) the $f_i(x)$ are distinct irreducible factors of $x^n - 1$. $\mathfrak{A}$ contains the polynomials $(x^n - 1)/f_i(x)$, bence contains the minimal ideals $\mathfrak{M}_i$, $i = 1, \cdots, \nu$, bence contains their union $\mathfrak{M}_i \cup \mathfrak{M}_2 \cup \cdots \cup \mathfrak{M}_\nu$. By (*ii*) the dimension of tbis union is the sum of the degrees of $f_1(x), \cdots, f_\nu(x)$ which by 2.1 is the dimension of $\mathfrak{A}$. Thus $\mathfrak{A} = \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \cdots \cup \mathfrak{M}_\nu$.

We note that this theorem is not true for even n.

Let $\theta_0, \theta_1, \cdots, \theta_{t-1}$ be the set of primitive idempotents of $\mathfrak{R}_n$.

Corollary 2.13:

(*i*) $\theta_i \cdot \theta_j = 0 \quad i \neq j$.

(*ii*) *Every idempotent of* $\mathfrak{R}_n$ *is of the form*

$$\sum_{i=0}^{t-1} \epsilon_i \theta_i ,$$

where ϵ_i *belongs to* V. *In particular,*

$$\sum_{i=0}^{t=1} \theta_i = 1.$$

Proof:

(*i*) Follows from 2.12 (*ii*) and 2.11 (*i*).

(*ii*) Since any ideal in $\mathfrak{R}_n$ is the union of minimal ideals, any idempotent can be obtained from the θ_i by repeated applications of 2.11 (*ii*). The product terms disappear by part (*i*) of this lemma. In particular

$$\mathfrak{R}_n \cdot 1 = \mathfrak{R}_n \cdot \left(\sum_{i=0}^{t-1} \theta_i \right).$$

*Lemma 2.14:** *If* μ_1, μ_2 *belong to the minimal ideal* $\mathfrak{M}$, *and* $\mu_1\mu_2 = 0$, *then either* $\mu_1 = 0$ *or* $\mu_2 = 0$.

Proof: Suppose that $\mu_2 \neq 0$. Consider the set Λ of elements m in $\mathfrak{M}$ such that $m\mu_2 = 0$. If $m_1, m_2 \in \Lambda$, so does $m_1 + m_2$; if $m \in \Lambda$ and $\mu \in \mathfrak{R}_n$, then $\mu m \in \Lambda$. Hence Λ is a subideal of $\mathfrak{M}$, so is either all of $\mathfrak{M}$ or the zero ideal. Let θ be the idempotent of $\mathfrak{M}$; then $\theta \cdot \mu_2 = \mu_2 \neq 0$; hence $\theta \in \Lambda$, and $\Lambda \neq \mathfrak{M}$. We must then have $\Lambda = 0$; consequently $\mu_1 = 0$.

It is clear that it will be advantageous to find the explicit forms of the primitive idempotents $\theta_i(x)$. Indeed if this were not easy the above theoretical results would have little practical value; however it is easy, and has in fact been done for all odd values of n through 1023. The method used is due to Prange,[7] and is described below.

Let $r = r_1, r_2, \cdots, r_m$ be a cycle of $\Sigma_2(n)$ and let η_r denote the polynomial $x^{r_1} + x^{r_2} + \cdots + x^{r_m}$ η_r is an idempotent, since squaring it simply rearranges the numbers which occur as exponents of x.

Lemma 2.14: The polynomial

$$\sum_{j=0}^{n-1} a_j x^a, \qquad a_j \in V,$$

is an idempotent if and only if it can be written as a sum of the η_r.

* Alternatively we might quote the well known theorem[4,5] that the minimal ideal $\mathfrak{M}$ is isomorphic to the Galois field $V[y]/f(y)$.

Proof: Clearly any sum of the η_r is idempotent. The "if" part of the lemma follows immediately from 2.2.

Lemma 2.15: The number of primitive idempotents of $\mathfrak{R}_n$ is the same as the number of cycles of $\Sigma_2(n)$.

Proof: Let s be the number of primitive idempotents. By 2.12 (*iii*) tbe number of ideals in $\mathfrak{R}_n$ is 2^s. Hence s is the number of cycles $\Sigma_2(n)$.

Any idempotent may be expressed as a linear combination of the η_r (wbich we can find easily) or as a linear combination of tbe primitive idempotents θ_j. The θ_j have the additional property that they are mutually orthogonal. In particular, each η_r is the sum of a subset of tbe θ_j; the problem is to split it into its components.

We observe tbat if S, T are nonempty subsets of tbe indices 0, $1, \cdots, t-1$, $S \neq T$, then

$$\left(\sum_{j \in S} \theta_j\right) \cdot \left(\sum_{j \in T} \theta_j\right) = \sum_{j \in S \cap T} \theta_j .$$

The product of two idempotents will contain fewer primitive idempotents than either factor.

Let t be the number of primitive idempotents. Then

$$1 = \sum_{j=0}^{t-1} \theta_j , \quad \text{and if} \quad 1 = \sum_{j=0}^{t-1} \xi_j$$

where the ξ_j are orthogonal idempotents, then the ξ_j are, except possibly in order, the same as the θ_j. We use this fact to set up an algorithm as follows:

Suppose that we have at some stage a decomposition of 1 into $\tau < t$ mutually orthogonal idempotents;

$$1 = \sum_{j=0}^{\tau-1} \xi_j , \; \xi_j^2 = 1, \; \xi_i \xi_j = 0 \qquad i \neq j.$$

Let ξ be an idempotent; set

$$\xi_j = \xi_j \xi + \xi_j(1 + \xi) = \xi_{j1} + \xi_{j2} j = 0, 1, \cdots, \tau - 1.$$

ξ_{j1}, ξ_{j2} are idempotent, and the new idempotents are mutually orthogonal. If the splitting is genuine (it may happen that $\xi_j = \xi$ or $\xi_j = 1 + \xi$, in which case no splitting takes places) tbe result is a decomposition of 1 into more than τ mutually ortbogonal idempotents.

To start the algorithm we set $1 = \eta_1 + (1 + \eta_1)$; the other η_j provide successive candidates for ξ. The computation is finished when there are t components in the decomposition of 1. Since the η_r are also a base for the idempotents of $\mathfrak{R}_n$, this stage must be reacbed by tbe time tbe set of η_r is exhausted.

The primitive idempotent $\theta_i(x)$ is the generating idempotent of a minimal ideal $\mathfrak{M}_i$; the orthogonal idempotent $1 + \theta_i(x)$ is the generating idempotent of a maximal ideal $\mathfrak{K}_i$: the generating factor $f_i(x)$ of $\mathfrak{K}_i$ is an irreducible factor of $x^n - 1$, and is the greatest common factor of $1 + \theta_i(x)$ and $x^n - 1$. In this way we can produce the parallel lists of primitive idempotents and irreducible factors of $x^n - 1$ referred to in Section I.

We return now to the automorphisms σ_q of $\mathfrak{R}_n$.

The set of automorphisms σ_q is an Abelian group, with $\sigma_{q_1}\sigma_{q_2} = \sigma_{q_1 q_2}$ defined in the usual way. It is isomorphic to the (multiplicative) group of integers mod n which are prime to n. Since σ_2 and its powers leave the idempotents of $\mathfrak{R}_n$ unchanged, we may, for our purposes, factor out this subgroup. In practice we choose one q from each cycle of $\Sigma_2(n)$ which contains integers prime to n. These q (and the associated σ_q) form a rather small Abelian group, whose structure may be found by hand, as illustrated for $n = 63$. It is worthwhile to find a set of generators for the group. One need only compute the effect of these generators on the set of primitive idempotents of $\mathfrak{R}_n$; it is then simple to calculate the effect of any automorphism on any ideal. Proposition VI is now established.

Proof of Proposition VII: Let $f_1(x)$ be the irreducible factor of $x^n - 1$ associated with the cycle $(1, 2, \cdots, 2^{m-1})$. v is an integer prime to n, and we wish to identify the polynomial $f_r(x)$ associated with the cycle $(v, 2v, \cdots, 2^{m-1}v)$. Since v is prime to n the two cycles will be the same length. $f_1(x)$ is the highest common factor of $1 + \theta_1(x)$ and $x^n - 1$. $1 + \theta_1(x)$ is thus divisible by the polynomial $(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{2m})$. Let u, prime to n, be such that $uv \equiv 1 \bmod n$. Then $(1 + \theta_1(x))\sigma_u = 1 + \theta_1(x^u)$ is divisible by

$$(x^u - \zeta)(x^u - \zeta^2) \cdots (x^u - \zeta^{2m})$$
$$= (x^u - \zeta^{uv})(x^u - \zeta^{2uv}) \cdots (x^u - \zeta^{2muv}),$$

which is divisible by $(x - \zeta^v)(x - \zeta^{2v}) \cdots (x - \zeta^{2mv})$.

Thus $f_r(x)$ divides $(1 + \theta_1(x))\sigma_u$ over $V(2^m)$, and since both polynomials have coefficients in V, $f_r(x)$ divides $(1 + \theta_1(x))\sigma_u$ over V. Hence $f_r(x)$ is the highest common factor of $(1 + \theta_1(x))\sigma_u$ and $x^n + 1$.

Spectra of Cyclic Alphabets

Let $a(x)$, $b(x)$ be the generating factor and reciprocal factor of an ideal $\mathfrak{A}$ in $\mathfrak{R}_n$. Let $b(x)$ belong to exponent e, where $n = e\alpha$, $\alpha > 1$. Let $\mathfrak{A}'$ be the ideal in $\mathfrak{R}_e$* with reciprocal polynomial $b(x)$.

* $\mathfrak{R}_e$ is the ring of polynomials mod $x^e - 1$.

Lemma 2.16: Every letter of $\mathcal{A}$ consists of α repetitions of a letter of $\mathcal{A}'$.

Proof: Let $a'(x) = (x^e - 1)/b(x)$ be the generating polynomial of $\mathcal{A}'$. Then

$$a(x) = (x^n - 1)/b(x) = \frac{x^n - 1}{x^e - 1} \cdot a'(x).$$

$$= \left(\sum_{i=0}^{\alpha} x^{n-ie}\right) a'(x).$$

Let $r(x)a'(x) = \sum_{i=0}^{\alpha} \alpha_i x^i$ (multiplication in $\mathcal{R}_e$) be a letter of $\mathcal{A}'$. With multiplication in $\mathcal{R}_n$, $\mathcal{A}$ contains

$$r(x)a(x) = \left(\sum_{1=0}^{\alpha} x^{n-ie}\right)\left(\sum_{i=0}^{e} \alpha_i x^i\right).$$

Hence each letter of $\mathcal{A}'$ gives rise to a letter of $\mathcal{A}$, which consists of α repetitions of the letter of $\mathcal{A}'$. It is evident that different letters of $\mathcal{A}'$ give rise to different letters of $\mathcal{A}$. Since tbe dimensions of $\mathcal{A}$ and $\mathcal{A}'$ are both equal to the degree of $b(x)$, all of $\mathcal{A}$ is obtained in this way.

Corollary 2.17: Let the spectrum of $\mathcal{A}'$ be $A'(i)$ $i = 0, \cdots, e$. The spectrum of $\mathcal{A}$ is given by the equations $A(\alpha i) = A'(i)$, $i = 0, \cdots, e$.

For example, let $n = 15$, and $b(x) = 1 + x + x^2$. $b(x)$ has exponent 3; $a'(x) = (x^3 + 1)/b(x) = 1 + x$; $a(x) = (1 + x^3 + x^6 + x^9 + x^{12})(1 + x)$. The ideals $\mathcal{A}'$, $\mathcal{A}$ are tabulated below.

0	1	2
0	0	0
1	1	0
0	1	1
1	0	1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1

Let T denote the cycle permutation $\omega \to \omega + 1 \pmod{n}$ of the numbers $0, 1, \cdots, n - 1$. T shall also denote the mapping $h(x) \to xh(x)$ (exponents mod n) of $\mathcal{R}_n$ onto itself. Clearly T^n is the identity mapping. If $\alpha \in \mathcal{A}$, the polynomials (or vectors) $\alpha T, \alpha T^2, \cdots, \alpha T^{n-1}$ also belong to $\mathcal{A}$. Tbe letters of $\mathcal{A}$ are divided into a number of nonoverlapping cycles; to construct $\mathcal{A}$ we need to know only one element from each cycle.

In fact it would seldom be useful to construct a picture of $\mathcal{A}$ in this way. We restrict ourselves to finding the spectrum of $\mathcal{A}$.

The set $\alpha, \alpha T, \cdots, \alpha T^{n-1}$ does not always contain n different letters. We denote by $\pi(\alpha)$ the number of different letters in this set; $\pi(\alpha)$ is called the *period* of α. The set

$$\alpha, \alpha T, \cdots, \alpha T^{\pi(\alpha)-1}$$

is then a complete cycle of $\mathcal{A}$, and the length of the cycle is $\pi(\alpha)$.

Let $r(x) \in \mathcal{R}_n$; let $a(x)$ be the highest common factor of $r(x)$ and $x^n - 1$, and let $b(x) = (x^n - 1)/a(x)$.

Lemma 2.18: The period of $r(x)$ is the exponent of $b(x)$.

Proof: Suppose $b(x)$ belongs to exponent e; set $a'(x) = [(x^e - 1)/b(x)]$, $r(x) = h(x)a(x)$, where $h(x)$ is relatively prime to $x^n - 1$. $r(x)(x^e - 1) = h(x)\cdot a(x)\cdot b(x)a'(x) = h(x)a'(x)(x^n - 1) = 0$. Hence $x^e r(x) = r(x)$, and the period of $r(x)$ is $\leqq e$.

Suppose that e' is the period of $r(x)$. Then $e' \leqq n$, and $r(x)(x^{e'} - 1) = 0$; in $V[x]$, $h(x)a(x)(x^{e'} - 1) = i(x)(x^n - 1) = i(x)a(x)b(x)$ where $i(x)$ is a polynomial in $V[x]$. $b(x)$ and $h(x)$ are relatively prime since $b(x)$ is a factor of $x^n - 1$. Thus $b(x)$ divides $(x^{e'} - 1)$, and $e' \geqq e$.

Proof of Proposition IX: $\pi(\theta_i)$ is the period of θ_i, and $\pi(m)$ the period of $m \in \mathcal{R}_n \cdot \theta_i$. Then $mx^{\pi(\theta_i)} = m\theta_i x^{\pi(\theta_i)} = m\theta_i = m$; hence $\pi(m) \leqq \pi(\theta_i)$. Also $0 = m\cdot(x^{\pi(m)} + 1) = m\theta_i\cdot(x^{\pi(m)} + 1) = m\theta_i\cdot\theta_i(x^{\pi(m)} + 1)$. By 2.13, since $m\theta_i \neq 0$, we must have $\theta_i(x^{\pi(m)} + 1) = 0$. Thus $\pi(\theta_i) \leqq \pi(m)$, so that $\pi(\theta_i) = \pi(m)$. By 2.18, $\pi(\theta_i)$ is the exponent of the irreducible polynomial $f_i(x)$.

If $n = 2^m - 1$, an irreducible polynomial $f(x)$ of exponent n has degree m, and a minimal ideal of period n contains just one cycle besides the zero cycle. The maximal ideal with generating factor $f(x)$ is a Hamming code (a close-packed code of minimum distance 3).[3] If n is not of this form, the minimal ideals of period n contain more than one cycle; it is then necessary to find several cycle representatives. No short-cut for doing this has been developed; the particular cases which have been studied have been solved by brute force.

If we have found a cycle representative for each cycle of $\mathcal{R}\theta_i$ and $\mathcal{R}\theta_j$, we can construct cycle representatives for $\mathcal{R}(\theta_i + \theta_j)$ with the help of the following lemmas.

Let $m \in \mathcal{R}\theta_i$, $n \in \mathcal{R}\theta_j$.

Lemma 2.19: $mT^\mu + nT^\nu = nT^{\mu'} + nT^{\nu'}$ if and only if $mT^\mu = mT^{\mu'}$ and $nT^\nu = nT^{\nu'}$.

Proof: The equation above may be written

$$mT^\mu - mT^{\mu'} = nT^\nu - nT^{\nu'}.$$

The left-hand side belongs to $\mathcal{R}\theta_i$ and the right-hand side to $\mathcal{R}\theta_j$. The intersection of these ideals is zero.

Let $\pi(m)$, $\pi(n)$ be the periods of m, n. Let H, h be respectively the least common multiple and highest common factor of these numbers.

Lemma 2.20: (Proof of Proposition X)*: The $\pi(m)\cdot\pi(n)$ elements $mT^\mu + nT^\nu$ are partitioned into h cycles of period H. The vectors $mT^\mu + n$, $\mu = 0, 1, \cdots, h - 1$ are in different cycles, and may be taken as cycle representatives.*

Proof: Let λ be the period of the vector $mT^{\mu} + nT^{\nu}$. Then

$$(mT^{\mu} + nT^{\nu})\, T^{\lambda} = mT^{\mu} + nT^{\nu},$$

and by 2.19 $\nu + \lambda \equiv \nu \bmod \pi(m)$ and $\mu + \lambda \equiv \mu \bmod \pi(n)$. Thus λ is divisible by both $\pi(m)$ and $\pi(n)$ and $\lambda = qH$, q an integer $\geqq 1$.

$mT^{\mu} + n$ and $mT^{\mu'} + n$ are in the same cycle if and only if

$$(mT^{\mu} + n)T^{\rho} = mT^{\mu'} + n,$$

or $\mu + \rho \equiv \mu' \bmod \pi(m)$ and $\rho \equiv 0 \bmod \pi(n)$. ρ and $\pi(m)$ are both divisible by h; hence $\mu - \mu' \equiv \rho \bmod \pi(m)$ implies that $\mu - \mu'$ is divisible by h. The h vectors $mT^{\mu} + n$, $\mu = 0, 1, \cdots, h - 1$ must be in different cycles.

Thus there are at least h different cycles, and the period of each is $\geqq H$. Since there are only $\pi(m)\pi(n) = hH$ elements altogether, the only possibility is that there are h cycles of period H.

We now return to Proposition V, which was omitted earlier. We restate the proposition as follows:

Theorem 2.21: Let $\mathfrak{M}_1$, $\mathfrak{M}_2$ be minimal ideals of $\mathfrak{R}_n$. The following three statements are equivalent:

(i) $\mathfrak{M}_1$, $\mathfrak{M}_2$ have the same spectrum.

(ii) $\mathfrak{M}_1$, $\mathfrak{M}_2$ have the same dimension and period.

(iii) There exists an automorphism σ_q of $\mathfrak{R}_n$ such that $\mathfrak{M}_1\sigma_q = \mathfrak{M}_2$.

Proof: We show that *(i)* $\Rightarrow$ *(ii)* $\Rightarrow$ *(iii)* $\Rightarrow$ *(i)*.

Let $A(s)$ be the number of letters of weight s in $\mathfrak{M}_i$. We prove that the period of $\mathfrak{M}_i$ is the highest common factor of $A(s)$, $s > 0$.

Suppose first that the period of $\mathfrak{M}_i$ is n; let 2^{k_i} be the total number of letters in $\mathfrak{M}_i$. The orthogonal complement of $\mathfrak{M}_i$ can contain no letters of weight 1 since it is a nontrivial cyclic alphabet. By Proposition VIII we obtain

$$\sum_{s=1}^{n} A(s) = 2^{k_i} - 1$$

$$\sum_{s=1}^{n} sA(s) = 2^{k_i - 1}n.$$

By the first equation, $k_1 = k_2$, so the dimensions of $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are equal. Since every cycle of $\mathfrak{M}_i$, except that containing the zero letter, is of length n, n divides each $A(s)$ for $s > 0$. By the second equation, any other common factor of $A(s)$ is a power of 2. By the first equation, there can be no such factor.

Suppose now that the period of $\mathfrak{M}_i$ is e_i, and $n/e_i = \alpha_i > 1$. By 2.16

and 2.17 there is a minimal ideal $\mathfrak{M}_i'$ in $\mathfrak{R}_{e_i}$ with period e_i and spectrum $A'(s)$ such that the spectrum of $\mathfrak{M}_i$ is given by $A(\alpha_i s) = A'(s)$. By the first part of the proof, e_i is the highest common factor of $A'(s)$, $s > 0$; hence e_i is the highest common factor of $A(\alpha_i s)$, $\alpha_i s > 0$.

(ii) $\Rightarrow$ *(iii)*. Suppose first that the period of $\mathfrak{M}_1$ and $\mathfrak{M}_2$ is n. Let $\mathfrak{M}_1$ correspond to the cycle $(1, 2, \cdots, 2^{m-1})$ of $\Sigma_2(n)$, and $\mathfrak{M}_2$ correspond to the cycle $(v, 2v, \cdots, 2^{m-1}v)$. v must be prime to n, since the irreducible polynomial associated with $\mathfrak{M}_2$ has exponent n. Choose u, prime to n so that $uv \equiv 1 \bmod n$. As in the proof of Proposition VII, $\mathfrak{M}_1\sigma_u = \mathfrak{M}_2$.

Suppose now that $\mathfrak{M}_i$ has exponent e, $i = 1, 2$, where $n/e = r > 1$. Let $\mathfrak{M}_1$, $\mathfrak{M}_2$ be associated with cycles $(r, 2r, \cdots, 2^{m'-1}r)$ and $(s, 2s, \cdots, 2^{m'-1}s)$. The lengths of these cycles are the same because $\mathfrak{M}_1$ and $\mathfrak{M}_2$ have the same dimension.

As in the proof of Lemma 2.5, $s = qr$, where q is prime to n. Applying again the proof of Proposition VII, we see that $\mathfrak{M}_1\sigma_q = \mathfrak{M}_2$.

(iii) $\Rightarrow$ *(i)*. If $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are equivalent they clearly have the same spectrum.

We have thus shown that minimal and maximal cyclic alphabets of $\mathfrak{R}_n$ which have the same spectrum are equivalent. It is not known whether this is true for other cyclic alphabets. However many cases have been found of cyclic alphabets which have the same spectrum but which are definitely not related by one of the automorphism σ_q.

CONCLUSION

Up to this time much of the theoretical work on binary cyclic alphabets has been concentrated on alphabets with block lengths of the form $n = 2^m - 1$. Such numbers become rather sparse as n increases. On the other hand, alphabets of long block length are important for actual use on the telephone network, and for such applications the block length, though large, is likely to be restricted to a narrow range. It is therefore expedient to develop economical procedures which will pick out the alphabets with preassigned properties if any such exist. The amount of information presented in this paper about the structure of the polynomial ring $\mathfrak{R}_n$ is no doubt formidable; it has, however, very practical applications.

REFERENCES

1. Slepian, D., A Class of Binary Signaling Alphabets, B.S.T.J., *35*, January, 1956, p. 203.
2. Elliott, E. O., Estimates of Error Rates for Codes on Burst Noise Channels, B.S.T.J., *42*, Sept., 1963, p. 1977.

3. MacWilliams, Jessie, A Theorem on the Distribution of Weights in a Systematic Code, B.S.T.J., *42*, Jan., 1963, p. 79.
4. Peterson, W. W., *Error Correcting Codes*, John Wiley and Sons, Inc., New York, 1961.
5. Van de Waerden, B. L., *Modern Algebra*, Julius Springer, Berlin, 1937.
6. Curtis, C. W., and Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*, John Wiley and Sons, Inc., New York, 1962.
7. Prange, E., An Algorithm for Factoring $x^n - 1$ over a Finite Field, Air Force Cambridge Research Center, AFCRC-TN-59-775.